

PAÍS DE LA UE · BÁLTICOS

Estonia: lo que los clientes esperan de sus proveedores

Estonia es chica y digital. Quien le presta servicios de TI está sujeto desde enero de 2026 a una obligación expresa de aviso según la ley estonia de ciberseguridad, también como proveedor en el exterior.

IDIOMA OFICIAL estonio	PRINCIPAL PUERTO DE CARGA Muuga (Port of Tallinn)	NIS2 Küberturvalisuse seadus, reformada, desde 01/01/2026	AUTORIDAD DE PROTECCIÓN DE DATOS Andmekaitse Inspektsioon
IVA 24 % tasa general			

Estonia como mercado para Sudamérica

Como destino para productos agrícolas sudamericanos, Estonia es un mercado chico. Vino, frutas, café y carne llegan en general a través de mayoristas que abastecen a varios países bálticos o también a Finlandia. Para los proveedores de servicios, el país es más interesante: organismos públicos y empresas trabajan en gran medida en forma digital, y el software se desarrolla a menudo con socios en el exterior. Un equipo en Montevideo o Córdoba que programa para un cliente en Tallin no llama la atención allí.

El mayor puerto de carga es Muuga, unos 17 kilómetros al este de Tallin. Perteneció al Port of Tallinn y tiene una terminal de contenedores. La mercadería sudamericana llega por lo general a través de un puerto de transbordo en Europa Occidental y luego en buque alimentador por el Báltico.

Qué es igual en toda la UE y qué rige a nivel nacional

Aduanas y normativa de productos son iguales en toda la UE. Desde el 01/05/2026 se aplica en forma provisional el pilar comercial del [Acuerdo UE-Mercosur](#). Si su mercadería se despacha a libre práctica en Róterdam, a partir de ahí es mercadería de la UE también en Estonia. Los detalles están en la [guía para exportar a la UE](#).

A nivel nacional se regulan el idioma de la información al consumidor (estonio), el IVA (tasa general del 24 %) y los envases. Estonia lleva un registro de envases según su ley de envases

(pakendiseadus); la obligación de declarar recae en quien introduce mercadería envasada en Estonia, en general su importador. Desde el 12/08/2026 rige además el Reglamento de envases de la UE (UE) 2025/40.

NIS2 en Estonia

Estonia no redactó una ley nueva: reformó su ley de ciberseguridad vigente (Küberturvalisuse seadus, KüTS). La reforma se publicó en el Riigi Teataja el 30/12/2025 y rige desde el 01/01/2026. Las empresas alcanzadas tuvieron que registrarse dentro de los tres meses a través del portal estatal eesti.ee. Para cumplir todas las obligaciones hay un período de transición de tres años; las obligaciones de notificación y el registro ya rigen.

Casi todo está a cargo de la Autoridad del Sistema de Información del Estado (Riigi Infosüsteemi Amet, RIA). Es autoridad de supervisión, punto de contacto central y CSIRT; los incidentes los gestiona su equipo CERT-EE. Los plazos siguen la directiva: primera notificación a más tardar a las 24 horas, notificación del incidente a las 72 horas.

Importante para los proveedores: según el § 8, apartado 1¹, de la KüTS, un proveedor de servicios que opera sistemas o aloja datos para una empresa alcanzada debe informar a su cliente sobre un incidente dentro de las 24 horas. Ante la autoridad responde su cliente, pero él va a incluir ese plazo en su contrato.

Los requisitos técnicos están en el Reglamento del Gobierno n.º 121. Las empresas más grandes deben implementar el estándar estonio de seguridad de la información E-ITS o presentar ante la RIA un certificado [ISO 27001](#) vigente. Para todas rigen medidas mínimas en nueve áreas, entre ellas, de forma expresa, la gestión de socios externos. Más sobre la directiva en la página de [NIS2](#).

Protección de datos y cadena de suministro

La autoridad de protección de datos es la Andmekaitse Inspektsioon, que supervisa el [RGPD](#) ([Reglamento General de Protección de Datos](#)) en Estonia. Para proveedores de servicios sudamericanos eso significa, en concreto: contrato de encargo de tratamiento, lista de medidas técnicas y organizativas y, para flujos de datos hacia su país, cláusulas contractuales tipo si no hay decisión de adecuación. La UE adoptó decisiones de adecuación para Argentina, Brasil y Uruguay; hacia esos países los datos pueden fluir sin cláusulas contractuales tipo. Para Chile, Colombia, Perú, Ecuador, Paraguay y Bolivia no hay decisión.

Estonia no tiene una ley propia de cadena de suministro. Las empresas estonias son en su mayoría demasiado chicas para la [CSDDD](#); los requisitos sobre derechos humanos y medio ambiente le van a llegar más bien a través de grandes grupos escandinavos que compran en los países bálticos.

Qué suelen exigir los clientes estonios

En servicios de TI, los clientes estonios preguntan temprano por la seguridad y el almacenamiento de datos: ¿dónde están los datos, quién tiene acceso, con qué rapidez avisa usted un incidente? Un certificado ISO 27001 ayuda por partida doble, porque el derecho estonio también lo reconoce como evidencia. Para prepararlo existe [Sightadel](#), que se desarrolla y se aloja en Alemania; su propia documentación de seguridad queda así también en la UE. Contratos y cuestionarios suelen estar en inglés.

En el comercio de alimentos rigen las evidencias habituales, es decir, un estándar reconocido por la GFSI como [IFS](#), [BRCGS](#) o [FSSC 22000](#) y, para café, cacao, soja, carne vacuna y madera, las obligaciones de diligencia debida del [EUDR](#).

Cómo proceder:

1. Verifique si su cliente estonio está alcanzado por la ley de ciberseguridad.
2. Establezca un canal de aviso que le permita informar incidentes al cliente con seguridad dentro de las 24 horas.
3. Documente sus medidas siguiendo las nueve áreas de las medidas mínimas estonias. En la plataforma GRC [Sightadel](#) puede cargarlas como un marco propio y asignar a cada área tareas y pruebas.
4. Considere un certificado ISO 27001 si atiende a varios clientes en Estonia.

Contactos útiles

ORGANISMO	PARA QUÉ
Maksu- ja Tolliamet	autoridad tributaria y aduanera de Estonia
Riigi Infosüsteemi Amet (RIA), CERT-EE	ciberseguridad y notificación de incidentes
ProChile, oficina de Estocolmo	competente también para Estonia, para exportadores chilenos
Enterprise Europe Network	búsqueda de socios y asesoramiento sobre derecho de la UE

No encontramos una cámara de comercio bilateral entre Estonia y un país sudamericano. Pregunte en la sección comercial de su embajada qué representación tiene competencia para Estonia; muchas

veces atiende también a todo el Báltico o a los países nórdicos.

FAQ

¿Como proveedor sudamericano debo notificar incidentes en Estonia?

No a la autoridad, pero sí a su cliente: dentro de las 24 horas, si usted opera sistemas o aloja datos para una empresa alcanzada (§ 8, apartado 1¹, de la KüTS).

¿Alcanza con ISO 27001 en lugar de E-ITS?

Sí. El Reglamento n.º 121 admite un certificado ISO/IEC 27001 vigente con un alcance adecuado como alternativa al estándar estonio E-ITS. Eso rige para su cliente; para usted como proveedor es la evidencia más sólida.

¿Cómo sé qué ve un cliente estonio de mis sistemas en internet?

Lo puede revisar desde afuera con [veyrisk](#). El servicio busca servicios abiertos, certificados vencidos y fallas en la configuración de DNS y correo, y prioriza cada hallazgo. El informe le sirve también para el cuestionario de seguridad del cliente.

¿Cuál es el IVA en Estonia?

La tasa general es del 24 %.

Fuentes · Actualizado: 11 de octubre de 2026

Küberturvalisuse seaduse muutmise seadus, RT I, 30.12.2025, 4: <https://www.riigiteataja.ee/akt/130122025004>

RIA: Uuest aastast laienes küberturvalisuse seadus: <https://www.ria.ee/uudised/uuest-aastast-laienes-kuberturvalisuse-seadus>

RIA, CERT-EE: Reporting a cyber incident: <https://www.ria.ee/en/cyber-security/handling-cyber-incidents-cert-ee/reporting-cyber-incident>

Andmekaitse Inspektsioon: <https://www.aki.ee/>

Comisión Europea: decisiones de adecuación: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Comisión Europea, Tu Europa: tipos de IVA: https://europa.eu/youreurope/business/taxation/vat/vat-rules-rates/index_es.htm

Port of Tallinn: Muuga Harbour: <https://www.ts.ee/en/muuga-harbour/>

Gobierno de Chile: Agregadurías en Suecia (ProChile): <https://www.chile.gob.cl/suecia/agregadurias-civiles>

Información general, no constituye asesoramiento legal. Prevalecen los textos oficiales.

PÓNGALO EN PRÁCTICA CON HERRAMIENTAS HECHAS EN ALEMANIA

 Sightadel

Sightadel guía a su equipo por NIS2: plantillas, tareas, evidencias y preparación de auditorías en un solo lugar. Desarrollado y alojado en Alemania, con paquete de consultoría opcional.

[Ver Sightadel →](#)

 veyrisk

veyrisk muestra lo que un atacante ve de su empresa desde fuera: servicios abiertos, certificados, vulnerabilidades conocidas. Puede presentar el informe a clientes europeos y auditores.

[Ver veyrisk →](#)

 valar

Valar es un firewall de hardware con software de neonotu. Protege oficinas y sedes y genera los registros que exigen NIS2 e ISO 27001.

[Ver Valar →](#)

Sightadel, veyrisk y Valar son productos de neonotu GmbH, empresa que opera MercoEU.

¿Qué parte de esto aplica a su empresa?

El diagnóstico UE gratuito se lo muestra en 10 minutos, según su sector y su país.

<https://www.mercoeu.com/es/diagnostico-ue>